Diese Kopfleiste bitte unbedingt ausfüllen!

Familienname, Vorname (bitte durch eine Leerspalte trennen)

Bereich	Berufsnummer	IHK-Nummer	Prüflingsnummer
7 0	1 2 0 2		
Sp. 1-2	Sp. 3-6	Sp. 7-9	Sp. 10-14

Termin: Mittwoch, 23. November 2022

IHK

Abschlussprüfung Winter 2022/23

1202

2 Analyse und Entwicklung von Netzwerken

Fachinformatiker
Fachinformatikerin
Systemintegration (AO 2020)

Teil 2 der Abschlussprüfung

4 Aufgaben
90 Minuten Prüfungszeit
100 Punkte

Bearbeitungshinweise

1. Bevor Sie mit der Bearbeitung der Aufgaben beginnen, überprüfen Sie bitte die **Vollständigkeit** dieses Aufgabensatzes. Die Anzahl der zu bearbeitenden Aufgaben ist auf dem Deckblatt links angegeben. Wenden Sie sich bei Unstimmigkeiten sofort an die Aufsicht, weil Reklamationen am Ende der Prüfung nicht anerkannt werden können.
2. Füllen Sie zuerst die **Kopfzeile** aus. Tragen Sie Ihren Familiennamen, Ihren Vornamen und Ihre Prüflings-Nr. in die oben stehenden Felder ein.
3. Lesen Sie bitte den **Text** der Aufgaben ganz durch, bevor Sie mit der Bearbeitung beginnen.
4. Halten Sie sich bei der Bearbeitung der Aufgaben genau an die **Vorgaben der Aufgabenstellung** zum Umfang der Lösung. Wenn z. B. vier Angaben gefordert werden und Sie sechs Angaben anführen, werden nur die ersten vier Angaben bewertet.
5. Tragen Sie die frei zu formulierenden **Antworten dieser offenen Aufgaben** in die dafür lt. Aufgabenstellung vorgesehenen Bereiche (Lösungszeilen, Formulare, Tabellen u. a.) des Arbeitsbogens ein.
6. Sofern nicht ausdrücklich ein Brief oder eine Formulierung in ganzen Sätzen gefordert werden, ist eine **stichwortartige Beantwortung** zulässig.
7. Schreiben Sie deutlich und gut lesbar. Ein nicht eindeutig zuzuordnendes oder **unleserliches Ergebnis** wird als **falsch** gewertet.
8. Zur Lösung der Rechenaufgaben darf ein nicht programmierter, netzunabhängiger **Taschenrechner** ohne Kommunikationsmöglichkeit mit Dritten verwendet werden.
9. Wenn Sie ein **gerundetes Ergebnis** eintragen und damit weiterrechnen müssen, rechnen Sie (auch im Taschenrechner) nur mit diesem gerundeten Ergebnis weiter.
10. Für **Hilfsaufzeichnungen** können Sie das in der Tasche beigelegte Konzeptpapier verwenden. Bewertet werden jedoch grundsätzlich nur Ihre Eintragungen in diesem Aufgabensatz.

Wird vom Korrektor ausgefüllt!

Bewertung

Für die Bewertung gilt die Vorgabe der Punkte in den Lösungshinweisen.

1. Aufg. ☐☐ (15 16) Punkte 2. Aufg. ☐☐ (17 18) Punkte 3. Aufg. ☐☐ (19 20) Punkte 4. Aufg. ☐☐ (21 22) Punkte

Prüfungszeit ☐ (23)
Die entsprechende Ziffer (1, 2 oder 3) finden Sie in der Abfrage nach der Prüfungszeit im Anschluss an die letzte Aufgabe.

Gesamtpunktzahl ☐☐☐ (24 25 26)

Prüfungsort, Datum

Unterschrift

Gemeinsame Prüfungsaufgaben der Industrie- und Handelskammern. Dieser Aufgabensatz wurde von einem überregionalen Ausschuss, der entsprechend § 40 Berufsbildungsgesetz zusammengesetzt ist, beschlossen. Hinweis: Im Interesse einer besseren Lesbarkeit wird in der Aufgabenstellung und in den Angaben zur Aufgabenstellung nur die männliche Form (generisches Maskulinum) verwendet. Die verkürzte Sprachform beinhaltet keine Wertung und die gewählten männlichen Formulierungen gelten uneingeschränkt auch für die weiteren Geschlechter.
Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2022 – Alle Rechte vorbehalten!

Korrekturrand

Die Aufgaben 1 bis 4 beziehen sich auf die folgende Ausgangssituation:

Sie arbeiten als Fachinformatiker bei der 1234-IT-Systemhaus GmbH. Für Ihren Arbeitgeber beraten Sie u. a. das Möbelhaus Rusticus GmbH. Den Netzwerkplan des Möbelhauses finden Sie in der perforierten Anlage.

Zwischen beiden Standorten existiert eine VPN-Verbindung. Außendienstmitarbeiter sind bereits teilweise mit Laptops ausgestattet, die über das Mobilfunknetz eine Datenverbindung zum Internet herstellen können. Für die Verbindung zum Hauptstandort soll zukünftig ebenfalls ein VPN eingesetzt werden.

1. Aufgabe (24 Punkte)

Sie sind damit beauftragt, das Netzwerk der Rusticus GmbH zu betreuen.

a) Für die DMZ wird das Netzwerk 203.0.113.64 /29 verwendet, welches Ihnen vom Provider zugewiesen wurde. Dieses Netzwerk soll überprüft werden.

aa) Der Router zum Internet (R-Rusticus-ext) soll die erste mögliche IP-Adresse im Netzwerk erhalten, der Router zum Firmennetz (R-Rusticus-int) die letzte mögliche IP-Adresse im Netzwerk.

Ergänzen Sie die folgende Tabelle. 2 Punkte

Router, Schnittstelle	IP-Adresse
R-Rusticus-ext, ETH	
R-Rusticus-int, ETH0	

ab) Geben Sie die vollständige Routingtabelle für den Router R-Rusticus-ext an. Die Subnetzmaske ist in Punkt-Dezimal-Schreibweise anzugeben. In der Spalte „Schnittstelle oder Next-Hop" ist, wann immer möglich, die Next-Hop-Adresse zu verwenden. 8 Punkte

Hinweis: Die Anzahl der Zeilen der Tabelle ist keine Vorgabe für die Anzahl der notwendigen Einträge.

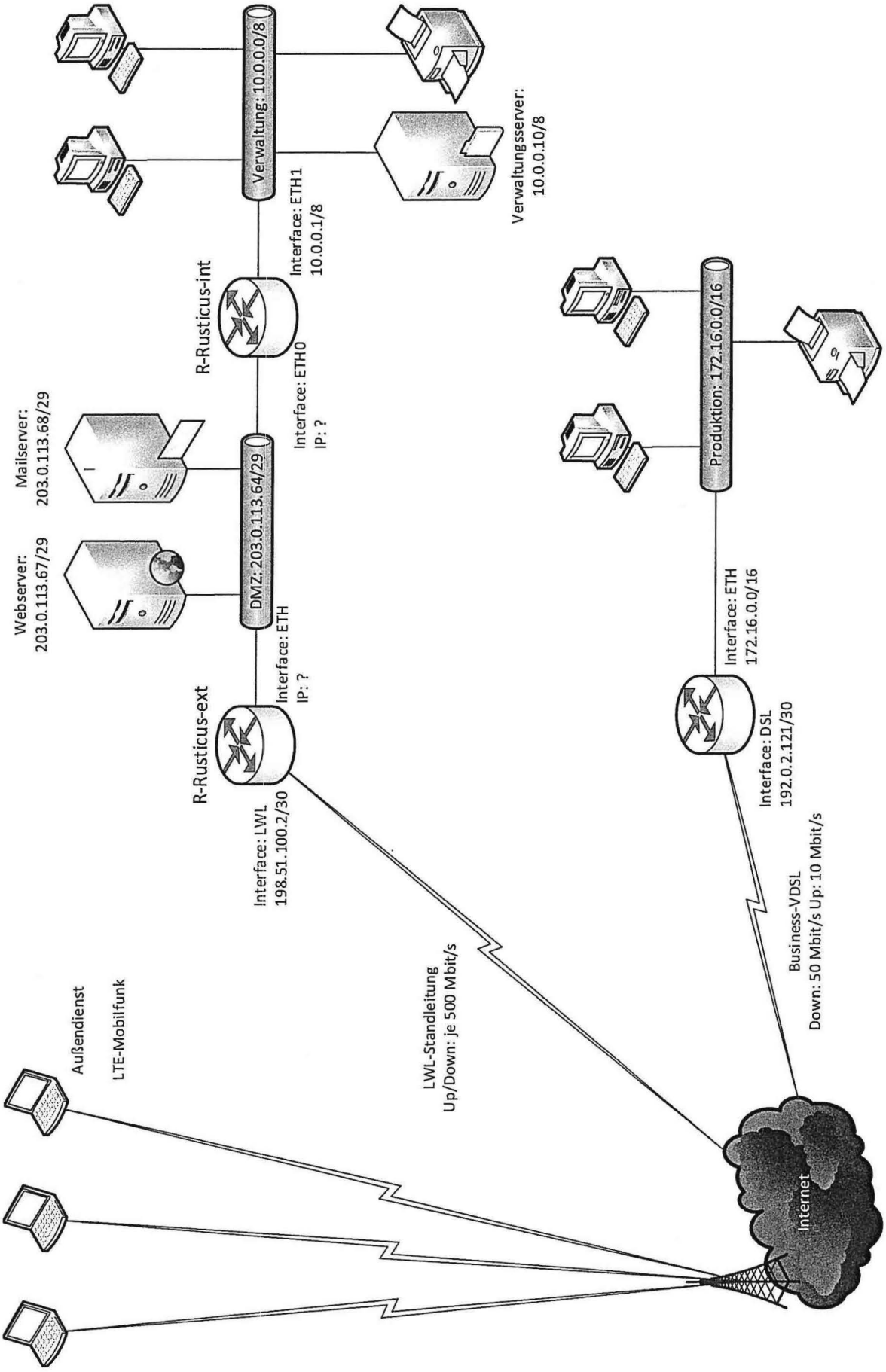
Netzwerk-ID	Subnetzmaske	Schnittstelle oder Next-Hop

b) Auf dem Router wird eine Firewall betrieben, zu deren Funktionsumfang auch SPI (Stateful Packet Inspection) zählt.

Erläutern Sie die Unterschiede einer Firewall mit aktivierter SPI-Funktion im Vergleich zu einer Firewall mit deaktivierter SPI-Funktion. 4 Punkte

Dieses Blatt kann an der Perforation aus dem Aufgabensatz herausgetrennt werden!

Anlage 1: Netzwerkplan



No.	Time	Source	Destination	Protocol	Length	Info
126	57041894	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	fd00::7642:7fff:fe0c:62f7	DNS	93	Standard query 0xd771 A www.google.de
127	57042168	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	fd00::7642:7fff:fe0c:62f7	DNS	93	Standard query 0x8737 AAAA www.google.de
128	57067860	10.0.0.101	8.8.4.4	DNS	73	Standard query 0x8737 AAAA www.google.de
129	57067860	10.0.0.101	8.8.4.4	DNS	73	Standard query 0xd771 A www.google.de
130	57083607	8.8.4.4	10.0.0.101	DNS	89	Standard query response 0xd771 A www.google.de A 142.251.36.163
131	57084949	fd00::7642:7fff:fe0c:62f7	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	DNS	121	Standard query response 0x8737 AAAA www.google.de AAAA 2a00:1450:4001:812::2003
132	57085082	fd00::7642:7fff:fe0c:62f7	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	DNS	109	Standard query response 0xd771 A www.google.de A 142.250.184.227
133	57094497	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	2a00:1450:4001:812::2003	ICMPv6	94	Echo (ping) request id=0x0001, seq=13, hop limit=128 (reply in 135)
134	57096359	8.8.4.4	10.0.0.101	DNS	101	Standard query response 0x8737 AAAA www.google.de AAAA 2a00:1450:4016:809::2003
135	57108031	2a00:1450:4001:812::2003	2001:db8:3726:1a00:70cd:9f70:a8a8:4627	ICMPv6	94	Echo (ping) reply id=0x0001, seq=13, hop limit=118 (request in 133)

Frame 126: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface \Device\NPF_{58E06F70-38E4-4725-85A1-79AB4C68C102}, id 0

Ethernet II, Src: hardware_5d:c2:ae (70:cd:cc:5d:c2:ae), Dst: distro_0c:62:f7 (76:42:7f:0c:62:f7)

Internet Protocol Version 6, Src: 2001:db8:3726:1a00:70cd:9f70:a8a8:4627, Dst: fd00::7642:7fff:fe0c:62f7

User Datagram Protocol, Src Port: 57616, Dst Port: 53

Domain Name System (query)

```
0000   76 42 7f 0c 62 f7 70 cd cc 5d c2 ae 86 dd 60 0e   ....b..!.]....`.
0010   59 59 00 27 11 ff 20 01 0d b8 37 26 1a 00 70 cd   YY.'.. ...7&..p.
0020   9f 70 a8 a8 46 27 fd 00 00 00 00 00 00 00 76 42   .p..F'........vB
0030   7f ff fe 0c 62 f7 e1 10 00 35 00 27 c5 7e d7 71   ....b....5.'.~.q
0040   01 00 00 01 00 00 00 00 00 00 03 77 77 77 06 67   ...........www.g
0050   6f 6f 67 6c 65 02 64 65 00 00 01 00 01            oogle.de.....
```

c) Stellen Sie für folgende Situationen passende Regeln für die Firewall auf, die den Traffic aus dem Internet regulieren: 10 Punkte

Korrekturrand

- Der Webserver soll von außen über HTTP erreichbar sein.
- Der Webserver soll von außen über HTTPS erreichbar sein.
- Andere Mailserver können Mails beim Mailserver über SMTP einliefern.
- Mails können mit dem Protokoll IMAP vom Mailserver abgerufen werden.
- Aller anderer Traffic aus dem Internet wird verworfen.

Aktion	Protokoll	Quelle	Ziel	Quellport	Zielport	Von Interface	Nach Interface

2. Aufgabe (23 Punkte)

Der Provider bietet für die Internetverbindung der Rusticus GmbH die Adressierung mittels IPv6 an. Auf den Netzwerkkomponenten wird daher zusätzlich das Protokoll IPv6 aktiviert.

Sie sollen die Netzwerkkonnektivität testen und zeichnen den Netzwerkverkehr für eine Überprüfung der Frames bzw. Pakete auf.

Sie geben an einem Client den Befehl `ping -n 1 www.google.de` ein.

Bildschirmausgabe:

```
C:\Users\user1>ping -n 1 www.google.de

Ping wird ausgeführt für www.google.de [2a00:1450:4001:812::2003] mit 32 Bytes
Daten:
Antwort von 2a00:1450:4001:812::2003: Zeit=13ms

Ping-Statistik für 2a00:1450:4001:812::2003:
    Pakete: Gesendet = 1, Empfangen = 1, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 13ms, Maximum = 13ms, Mittelwert = 13ms
```

Sie analysieren den Netzwerkverkehr und kontrollieren die Aufzeichnung der dazugehörigen Frames No. 126 bis 135 (siehe Rückseite perforierte Anlage).

a) Beschreiben Sie den Grund, weshalb der Client zuerst eine DNS-query (DNS-Abfrage) startet. 3 Punkte

b) Ermitteln Sie den Rückgabewert der Antwort auf die DNS-Anfrage aus Frame No. 126. 4 Punkte

Fortsetzung 2. Aufgabe →

Fortsetzung 2. Aufgabe

Korrekturrand

c) Bestimmen Sie die lokale IPv4-Adresse und die genutzte IPv6-Adresse des Clients. 4 Punkte

IPv4	
IPv6	

d) Ermitteln Sie die IP-Adresse des genutzten lokalen DNS-Servers. 3 Punkte

e) Begründen Sie, warum der PING an die IP-Adresse 2a00:1450:**4001:812**::2003 und nicht an die Adresse 2a00:1450:**4016:809**::2003 gesendet wurde. 3 Punkte

f) Berechnen Sie mithilfe der Werte aus den aufgezeichneten Frames die Anzahl der Router (hops), über die die ping-Antwort gelaufen ist.

3 Punkte

g) Beschreiben Sie einen möglichen Grund, warum Sie mehrere IPv4- und IPv6-Adressen für `www.google.de` als Antworten erhalten haben.

3 Punkte

3. Aufgabe (27 Punkte)

Korrekturrand

Der Zugriff der Außendienstmitarbeiter auf den Server der Rusticus GmbH soll über TLS-Verbindungen erfolgen.

a) Nennen Sie zwei Eigenschaften, welche eine TLS-Verbindung sicherer machen als eine normale TCP/IP-Verbindung. 4 Punkte

b) Im August 2018 wurde die Version TLS1.3 in RFC8446 verabschiedet. Innerhalb Ihres Teams wird zurzeit beraten, ob für die Zugänge der Rusticus-Außendienstmitarbeiter ausschließlich TLS1.3 zugelassen wird, oder ob auch Verbindungen nach TLS1.2 noch akzeptiert werden.

Begründen Sie anhand von drei Argumenten aus dem RFC8446, warum Verbindungen nach TLS1.2 für den Online-Zugang bei der Rusticus GmbH nicht mehr zugelassen werden sollten. 9 Punkte

RFC8446 (Auszug):

> **Major Differences from TLS 1.2**
>
> The following is a list of the major functional differences between TLS 1.2 and TLS 1.3. It is not intended to be exhaustive, and there are many minor differences.
>
> - The list of supported symmetric encryption algorithms has been pruned of all algorithms that are considered legacy.
>
> - Static RSA and Diffie-Hellman cipher suites have been removed; all public-key based key exchange mechanisms now provide forward secrecy.
>
> - All handshake messages after the ServerHello are now encrypted.
>
> - Session resumption has been replaced by a single new PSK exchange.

Vokabel-Hilfe:
exhaustive – erschöpfend, vollständig
to prune (of) – bereinigen, säubern von
resumption – Fortsetzung, Wiederaufnahme

Fortsetzung 3. Aufgabe →

Korrekturrand

c) Zur Authentifizierung des Servers werden bei SSL/TLS-Verbindungen Zertifikate nach X.509 eingesetzt, die von einer sogenannten CA (Certificate Authority) signiert sein müssen. Diese CA kann sowohl intern (self-signed), als auch von einer externen Zertifizierungsstelle betrieben werden.

Entscheiden Sie sich für eines der beiden Verfahren (interne CA/externe CA), und begründen Sie die Entscheidung anhand von zwei Argumenten. 6 Punkte

d) Nach erfolgreichem SSL/TLS-Verbindungsaufbau ist lediglich der Server der Rusticus GmbH gegenüber dem Endgerät des Mitarbeiters authentifiziert. Eine umgekehrte Authentifizierung steht noch aus. Diskutiert werden aktuell vier verschiedene Verfahren, um den Client gegenüber dem Server zu authentifizieren.

1. Username + Passwort
2. Username + Passwort + Client-Zertifikat
3. Username + Passwort + Krypto-Smart-Card
4. Username + Passwort + OneTimePassword (Authenticator-App)

Erläutern Sie zu jedem Verfahren einen Vorteil, der für den Einsatz des jeweiligen Verfahrens spricht. 8 Punkte

Verfahren	
1	
2	
3	
4	

4. Aufgabe (26 Punkte)

Korrekturrand

a) Im Möbelhaus Rusticus sind 100 VoIP-Telefonanschlüsse vorhanden. Der VoIP-Server befindet sich in der Cloud. Das bedeutet, dass auch interne Gespräche zwischen den Nebenstellen über den Internetanschluss laufen. Die Cloud-Telefonanlage nutzt standardmäßig den Codec G.722 (64 kBit/s). Der Protokolloverhead beträgt 10 %.

Berechnen Sie die benötigte Bandbreite in kBit/s, wenn gleichzeitig fünf Gespräche intern und fünfzehn Gespräche extern geführt werden. 5 Punkte

b) Für Videokonferenzen nutzt das Möbelhaus Rusticus Software, über die Sie im Datenblatt folgende Hinweise finden:

```
This software is designed to give the best audio, video, and content sharing
experience regardless of your network conditions. That said, when bandwidth
is insufficient, our product prioritizes audio quality over video quality.
Where bandwidth isn't limited, our product optimizes media quality, including
high-fidelity audio, up to 1080p video resolution, and up to 30fps (frames
per second) for video and content.
This table describes how we use bandwidth. Our software is always conser-
vative on bandwidth utilization and can deliver HD video quality in under
1.5Mbps. The actual bandwidth consumption in each audio/video call or meeting
will vary based on several factors, such as video layout, video resolution,
and video frames per second. When more bandwidth is available, quality and
usage will increase to deliver the best experience.
```

ba) Erläutern Sie, was geschieht, wenn die Bandbreite für die gleichzeitige Audio- und Videoübertragung nicht ausreicht. 3 Punkte

bb) Nennen Sie drei Faktoren, von denen die aktuell genutzte Bandbreite abhängt. 3 Punkte

Fortsetzung 4. Aufgabe →

Korrekturrand

c) Das Möbelhaus Rusticus führt derzeit regelmäßig Videokonferenzen durch, an denen maximal zehn Personen teilnehmen.

Wie hoch ist der hierbei entstehende zusätzliche Traffic auf dem Internetanschluss im Upload und Download, wenn die empfohlene Bandbreite genutzt wird? 2 Punkte

Modality	**Bandwidth requirements (bitrate kBit/s up/down)**		
	Minimum	**Recommended**	**Best performance**
Audio			
One-to-one	10/10	58/58	76/76
Meetings	10/10	58/58	76/76
Video			
One-to-one	150/150	1.500/1.500	4.000/4.000
Meetings	150/200	2.500/4.000	4.000/4.000

d) Das Möbelhaus Rusticus bietet seinen Kunden 3D-Animationsfilme an, die die fertige Küche zeigen. Die Filme dauern jeweils 5 Minuten und werden den Kunden zum Download angeboten. Die Videos haben durchschnittlich eine Größe von 34 MiB pro Minute. Der Kunde verfügt über einen ADSL-Anschluss (Download: 16 Mbit/s, Upload: 2 Mbit/s).

Wie lange dauert die Übertragung eines solchen Videoclips mindestens?

Das Ergebnis ist auf volle Sekunden aufzurunden. 4 Punkte

e) Die Rusticus GmbH nutzt für die Datenübertragung QoS.

Erläutern Sie die Funktionsweise von QoS und welche Auswirkungen für den Benutzer man sich durch den Einsatz von QoS bei der Übertragung von Telefonie- und Videodaten verspricht. 4 Punkte

f) In der Kommunikation mit einem Zulieferer bedient sich das Möbelhaus Rusticus nach wie vor der Dokumentenübertragung per Telefax. Seit der Umstellung auf VoIP berichtet das mit dem Fax-Versand betraute Personal immer wieder von Schwierigkeiten beim Versand sowie dem Erhalt von Fax-Dokumenten, insbesondere von unvollständigen Übertragungen, wenn mehrere Seiten übermittelt werden sollen.

Korrekturrand

Beschreiben Sie eine mögliche Ursache, die im Zusammenhang mit VoIP-Übertragungsprotokollen zu diesen Schwierigkeiten beim Versand bzw. Empfang von Fax-Dokumenten führen kann. 5 Punkte

PRÜFUNGSZEIT – NICHT BESTANDTEIL DER PRÜFUNG!

Wie beurteilen Sie nach der Bearbeitung der Aufgaben die zur Verfügung stehende Prüfungszeit?

[1] Sie hätte kürzer sein können.
[2] Sie war angemessen.
[3] Sie hätte länger sein müssen.

Abschlussprüfung Winter 2022/23
Lösungshinweise

Fachinformatiker/Fachinformatikerin
Systemintegration (AO 2020)
1202

2 Analyse und Entwicklung von Netzwerken

Teil 2 der Abschlussprüfung

Allgemeine Korrekturhinweise

Die Lösungs- und Bewertungshinweise zu den einzelnen Handlungsschritten sind als Korrekturhilfen zu verstehen und erheben nicht in jedem Fall Anspruch auf Vollständigkeit und Ausschließlichkeit. Neben hier beispielhaft angeführten Lösungsmöglichkeiten sind auch andere sach- und fachgerechte Lösungsalternativen bzw. Darstellungsformen mit der vorgesehenen Punktzahl zu bewerten. Der Bewertungsspielraum des Korrektors (z. B. hinsichtlich der Berücksichtigung regionaler oder branchenspezifischer Gegebenheiten) bleibt unberührt.

Zu beachten ist die unterschiedliche Dimension der Aufgabenstellung (nennen – erklären – beschreiben – erläutern usw.).

Für die Bewertung gilt folgender Punkte-Noten-Schlüssel:

Note 1	=		100 – 92 Punkte	Note 2	=	unter	92 – 81 Punkte
Note 3	=	unter	81 – 67 Punkte	Note 4	=	unter	67 – 50 Punkte
Note 5	=	unter	50 – 30 Punkte	Note 6	=	unter	30 – 0 Punkte

Die Vervielfältigung, Verbreitung und öffentliche Wiedergabe der Prüfungsaufgaben und Lösungen ist nicht gestattet. Zuwiderhandlungen werden zivil- und strafrechtlich (§§ 97 ff., 106 ff. UrhG) verfolgt. – © ZPA Nord-West 2022 – Alle Rechte vorbehalten!

1. Aufgabe (24 Punkte)

aa) 2 Punkte

Router, Schnittstelle	IP-Adresse
R-Rusticus-ext, ETH	203.0.113.65
R-Rusticus-int, ETH0	203.0.113.70

ab) 8 Punkte

Netzwerk-ID	Subnetzmaske	Schnittstelle oder Next-Hop
203.0.113.64	255.255.255.248	ETH
198.51.100.0	255.255.255.252	LWL
10.0.0.0	255.0.0.0	203.0.113.70
0.0.0.0	0.0.0.0	198.51.100.1

b) 4 Punkte
SPI sorgt dafür, dass Antworten für erlaubten Traffic für einen bestimmten Zeitraum automatisch ebenfalls die Firewall passieren dürfen, ohne dass der Admin dafür manuell Regeln aufstellen muss.

Andere Formulierungen möglich.

c) 10 Punkte (2 Punkte pro korrekter Regel)

Aktion	Protokoll	Quelle	Ziel	Quellport	Zielport	Von Interface	Nach Interface
Permit	TCP	any	203.0.113.67/32	any	80	LWL	ETH
Permit	TCP	any	203.0.113.67/32	any	443	LWL	ETH
Permit	TCP	any	203.0.113.68/32	any	25	LWL	ETH
Permit	TCP	any	203.0.113.68/32	any	143	LWL	ETH
Deny	IP	any	any				

2. Aufgabe (23 Punkte)

a) 3 Punkte
Der Client hat keine IP-Adresse für `www.google.de` zwischengespeichert, darum muss erst die IP-Adresse für `www.google.de` abgefragt werden.

Andere Antworten sind möglich.

b) 4 Punkte
(In Zeile 126 wird ein **A** Eintrag (**IPv4**) über einen IPv6-DNS-Server abgefragt. Die Antwort kommt mit Frame No. 132. Der relevante Rückgabewert ist in INFO enthalten:)
`........ A www.google.de A 142.250.184.227`

c) 4 Punkte
IPv4: **10.0.0.101** (2 Punkte)
IPv6: **2001:db8:3726:1a00:70cd:9f70:a8a8:4627** (2 Punkte)

d) 3 Punkte
fd00::7642:7fff:fe0c:62f7 (Die einzige neben der des Clients genutzten lokalen Adresse (8.8.4.4) ist öffentlich und nicht lokal.)

e) 3 Punkte
Die Antwort mit der Adresse 2a00:1450:4016:809::2003 ist erst nach dem abgesendeten ICMPv6-request eingetroffen. Der Zeitstempel (Time) ist höher, also später in der Zeit angesiedelt.

f) 3 Punkte
128 – 118 = 10
(Hinweis: Gesendet werden icmp Nachrichten i. d. R. mit einem hop limit von 128. Beim Durchlaufen des Pakets in einem Router wird das hop limit um 1 erniedrigt.
In der ping-Antwort (Echo reply Paket 135) ist das hop limit mit 118 angegeben.
Die Differenz beträgt 10.)

g) 3 Punkte
- Lastverteilung über DNS
- Es wurden unterschiedliche DNS-Server angefragt (IPv4 und IPv6).
- Der lokale IPv6-DNS-Server (Forwarder) hat andere (ältere) DNS-Einträge zwischengespeichert.
- Der öffentliche IPv4-DNS-Server (8.8.4.4) hat andere (neuere) DNS-Einträge.
- Der lokale DNS-Server nutzt weitere DNS-Forwarder (z. B. beim Provider) für DNS-Abfragen.

Weitere Antworten sind möglich.

3. Aufgabe (27 Punkte)

a) 4 Punkte
- Authentifizierung des Servers beim Client
- Vertraulichkeit der übertragenen Daten
- Schutz der übertragenen Daten vor Manipulation

b) 9 Punkte
Nachteile von TLS 1.2:
- TLS1.2 lässt Schlüsseltausch ohne PFS zu
- TLS1.2 enthält veraltete kryptografische Bibliotheken
- TLS1.2 lässt Teile des Handshakes unverschlüsselt
- TLS1.2 ermöglicht Angriffe durch „session resumption"

Andere Antworten sind möglich, auch möglich: Vorteile von TLS 1.3 nennen.

c) 6 Punkte
Intern:
- Eigene Kontrolle über Root-Keys
- Kontrolle des Verfahrens
- Ausstellen von neuen Zertifikaten sofort möglich

Weitere Antworten sind möglich.

Extern:
- Wahrscheinlich mehr Erfahrung bei externem Anbieter
- Keine eigene Infrastruktur notwendig
- Hinterlegen der public-keys der CA erfolgt über SW-Updates

Weitere Antworten sind möglich.

d) 8 Punkte
1. einfach zu implementieren; Anmeldung ist von beliebigen Endgeräten aus möglich
2. 2FA; Anmeldung lediglich an Geräten möglich, die über die Zertifikatsdatei verfügen
3. 2FA; 2ter Faktor an Hardware (= Besitz) gebunden
4. 2FA, keine Anschaffungskosten für zweiten Faktor, einfacher zu implementieren, da jeder User die App selbst installieren kann

Andere Antworten sind möglich.

4. Aufgabe (26 Punkte)

a) 5 Punkte
Berechnung:
Fünf Gespräche intern = 10 Teilnehmer * 64 kBit/s = 640 kBit/s (2 Punkte)
Fünfzehn Gespräche Extern = 15 Teilnehmer * 64 kBit/s = 960 kBit/s (2 Punkte)
Zusammen 1.600 kBit/s * 1,1 (Overhead) = 1.760 kBit/s (1 Punkt)

Folgefehler berücksichtigen, andere Rechenwege sind möglich.

ba) 3 Punkte
Das bedeutet, wenn die Bandbreite unzureichend ist, priorisiert die Software Audio-Qualität höher als Video-Qualität.

bb) 3 Punkte
Video-Layout, Video-Auflösung, und Video frames per second (fps)

c) 2 Punkte
10 * 2.500 kbit/s upload = 25.000 kbit/s
10 * 4.000 kbit/s download = 40.000 kbit/s

d) 4 Punkte
Maßgeblich ist das Download-Limit des ADSL-Anschlusses.

34 MiB/min * 5 min = 170 MiB
170 MiB * 1.024 (KB pro MB) = 174.080 KiB * 1.024 (Byte pro KB) = 178.257.920 Byte * 8 Bit pro Byte = 1.426.063.360 Bit
1.426.063.360 Bit / 16.000.000 Bit/s = 89,12896 Sek. = 90 Sek.

Berechnung und Ergebnis 90 Sek.

e) 4 Punkte
Quality of Service priorisiert die Daten von Echtzeitanwendungen. Auswirkungen: weniger Störungen, weniger Aussetzer, andere Antworten möglich.

f) 5 Punkte
VoIP ist auf Sprachübertragung optimiert, nicht auf Datenübertragung. Ein Sprach-Codec muss ggf. Datenverlust ausgleichen können, was bei Sprache ungehört bleibt, bei Fax aber zum Abbruch der Übertragung führen kann.

Weitere Lösungen sind möglich.